

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND  
SOUTHERN DIVISION**

**IN RE: MARRIOTT INTERNATIONAL  
CUSTOMER DATA SECURITY BREACH  
LITIGATION**

**THIS DOCUMENT RELATES TO:**  
Case No. 19-cv-654

MDL No. 19-md-2879

JUDGE PAUL W. GRIMM

**REPLY IN SUPPORT OF DEFENDANTS’  
MOTION TO DISMISS THE CITY OF  
CHICAGO’S AMENDED COMPLAINT**

**I. THIS ACTION EXCEEDS THE CITY’S HOME-RULE POWERS.**

This action stretches the city’s consumer protection ordinance beyond its breaking point. Home rule is meant to allow municipalities to address “problems that are local in nature,” not intervene in state or national affairs. *Village of Bolingbrook v. Citizens Utils. Co. of Ill.*, 632 N.E.2d 1000, 1002 (Ill. 1994). Of all the home-rule cases the parties cite in their briefing, not one involves a matter so clearly beyond local concern as the Marriott cyberattack—an incident the city labels as the “second largest data breach in history.” (Am. Compl. ¶ 1.) The city also seeks to regulate and punish alleged conduct that occurred beyond its borders, and its claims fail for that reason too. *See Hertz Corp. v. City of Chicago*, 77 N.E.3d 606, 609-10 (Ill. 2017).

To be clear, Marriott does not seek to invalidate the ordinance, but only to prevent its application here. In fact, the ordinance on its face disavows “the regulation of any business to the extent that such regulation is not permitted under the statutory or home rule powers of the city.” Chi., Ill., Mun. Code § 2-25-090(a). Thus, this lawsuit is barred not only by the constitutional limits on the city’s home-rule authority but by the terms of the ordinance as well.

**A. This Action Reaches Beyond the City’s Local Concerns.**

**1. The Marriott cyberattack is not a local problem.**

The city argues that home-rule units are permitted to regulate in an area “even though the

problem at issue also existed outside the home rule unit's borders.” (Pl. Opp’n 13, ECF No. 40.) But the Marriott cyberattack did not merely “also exist[]” outside Chicago—it *originated* outside Chicago and the city alleges its impact was felt throughout the United States and beyond. (See Am. Compl. ¶ 1, ECF No. 29; Defs. Br. 11, ECF No. 33.) In fact, in its response the city does not dispute that Marriott’s data security practices occurred outside the city. Nor does it identify how the incident affected Chicago differently than any other major city.

The city’s argument runs headlong into the holding of *City of Des Plaines v. Chicago & North Western Railway Co.*, 357 N.E.2d 433 (Ill. 1976). There the Supreme Court struck down an ordinance pertaining to train noise because it “was designed to regulate unwanted noise emissions affecting Des Plaines residents *whether or not the noise pollution originated within that municipality.*” *Id.* at 435 (emphasis added). In so holding, the court rejected the central thesis advanced by the city here—namely, that the city is empowered to regulate and punish data breaches allegedly affecting its residents regardless of where those breaches occur.

That is not to say all data breaches are categorically beyond the city’s reach. The story might be different, say, if a local hotel disseminated the personal data of its Chicago guests. The city then might well be justified in arguing its local interests prevail and its ordinance applies.

The Supreme Court drew a similar distinction in *Bolingbrook*, where it upheld a village’s home-rule authority to fine a public utility for improper sewer discharges. 632 N.E.2d at 1003. In classifying the problem as local, the court explained “this case deals with isolated incidents of a system malfunction” where the “main impact” was felt in the village, rather than throughout the state. *Id.* at 1003. The court went on to hold: “Where the impact of a problem is confined to an isolated area, and there is no evidence that the particular problem is common throughout the State, the ‘nature and extent of the problem’ are local in dimension.” *Id.*

The noise pollution at issue in *Des Plaines* provides an especially useful analogy. In limiting a city's authority to assess fines in this area, the Supreme Court contrasted "an irate motorist sounding his horn" with "noise emissions from trains in transit." 357 N.E.2d at 435. In other words, while some sources of noise pollution are local, others are not. For example, in *Village of Caseyville v. Cunningham*, 484 N.E.2d 499, 501 (Ill. App. Ct. 1985), the court upheld a municipal fine for a noisy parked truck, explaining: "Not every noise problem will be of statewide concern. We cannot find that loud mufflers, squealing tires or barking dogs are of such statewide concern." The noise from passing trains, in contrast, "extends beyond its source" into other jurisdictions, and the Supreme Court thus held that regulating it "is a matter requiring regional, if not statewide, standards and controls." *Des Plaines*, 357 N.E.2d at 435.

The city's own cases are in accord. Home-rule authority was upheld in those cases because the regulated conduct took place within the municipality and—to use the Supreme Court's language in *Bolingbrook*, 632 N.E.2d at 1003—because the "main impact" arising from that conduct was felt within the municipality as well. *See Scadron v. City of Des Plaines*, 606 N.E.2d 1154, 1157-58 (Ill. 1992) (ordinance regulating billboards within city's borders); *Kalodimos v. Village of Morton Grove*, 470 N.E.2d 266, 268-69 (Ill. 1984) (banning possession of handguns within village); *Accel Entm't Gaming, LLC v. Village of Elmwood Park*, 46 N.E.3d 1151, 1153, 1160 (Ill. App. Ct. 2015) (imposing registration, licensing, and fee requirements on video gambling machines within village); *Park Pet Shop, Inc. v. City of Chicago*, 872 F.3d 495, 497 (7th Cir. 2017) (limiting sources from which pet stores could obtain animals for sale in city).

The city's attempt to enforce its ordinance here is not of the same ilk. The city is purporting to regulate data security practices that took place beyond its borders and that allegedly affected individuals in cities and states throughout the country. And while the city focuses on the

alleged impact to Chicagoans and argues (incorrectly) that some of the challenged conduct occurred within its borders (Opp’n 13, 17), the same can be said of the train noise at issue in *Des Plaines*, some of which emanated from a railyard in Des Plaines, 357 N.E.2d at 434. In fact, the problem the city seeks to regulate here is far more removed from local concerns than the passing trains in *Des Plaines*, or the feral cats in *County of Cook v. Village of Bridgeview*, 8 N.E.3d 1275, 1279-80 (Ill. App. Ct. 2014). The courts’ reasons for limiting home-rule authority in those cases thus applies with much greater force here.

## **2. The City’s Ordinance Is Not a Local Solution.**

The city extolls its ordinance as “precisely” the type of “local solution” on which home rule is predicated. (Opp’n 14.) But cutting and pasting the state’s consumer and data protection statutes does not comport with the Supreme Court’s vision of a “local solution and reasonable experimentation to meet local needs, free from veto by voters and elected representatives of other parts of the State[.]” *See Kalodimos*, 470 N.E.2d at 274. Instead, it smacks of a cynical ploy to use local concerns as a pretext to raise municipal revenue—an inference that is only strengthened by the city’s repeated references to similar lawsuits it has recently filed over major data breaches suffered by Uber and Equifax. (*See* Opp’n 2, 8, 14, 17-20.)

## **3. Regulating the Marriott Cyberattack Is a State or National Issue.**

The city claims the state lacks a vital interest in regulating this cyberattack. (Opp’n 14.) But home-rule authority extends only to “problems that are local in nature rather than State *or* national.” *Bolingbrook*, 632 N.E.2d at 1002 (emphasis added). Thus, the inquiry is not focused solely on the state’s interest, but on whether the issue calls for regulation at a higher level of government than the city. And that is clearly true here, where both the alleged conduct and the alleged impact sought to be regulated extends far beyond the city’s borders. *See Des Plaines*, 357 N.E.2d at 435; *Bridgeview*, 8 N.E.3d at 1279.

In any event, by enacting PIPA, the state of Illinois *has* expressed its interest in regulating data security matters. *See Des Plaines*, 357 N.E.2d at 436 (holding that Illinois’s EPA “while not determinative” of the issue, “does provide further evidence of the recognition of noise pollution as a matter of statewide concern”); *Bridgeview*, 8 N.E.3d at 1279 (“The General Assembly, through the Animal Control Act, has determined that the issues of animal control, overpopulation, and the control of rabies are more effectively addressed at the county level.”).

The city counters by arguing that *Des Plaines* and *Bridgeview* should apply only where “conflicting” ordinances or state laws are at issue. (Opp’n 16-19.) But there was no such conflict in *Des Plaines*. Although the defendant argued that the state’s EPA preempted the city’s ordinance, the court found that regulating train noise was “not within the [city’s] home rule power” without resolving the preemption issue. 357 N.E.2d at 435-36. Instead, in reaching its decision, the court held, as noted above, that the existence of the Illinois EPA was “further evidence” of the state’s interest in regulating noise pollution. *Id.* at 436. And the same can be said in this case, where PIPA reflects the state’s interest in regulating data security.<sup>1</sup>

The city’s attempt to rely on references to *Des Plaines* and *Bridgeview* in subsequent decisions also falls flat. Despite the city’s inaccurate discussion of *County of Cook v. John Sexton Contractors Co.*, 389 N.E.2d 553, 558-59 (Ill. 1979), the court there explained its reasons for striking down the noise pollution ordinance in *Des Plaines* as follows: “although the immediate facts dealt with noise emission within the city, the city admitted that the ordinance was intended to control emissions originating beyond its boundaries.” *See also Kalodimos*, 470

---

<sup>1</sup> As the city points out, we mistakenly cited the *Kalodimos* dissent for the proposition that a state regulatory scheme is “evidence that a subject is recognized as a matter of statewide concern.” But the city does not mention that the same point has been made by Illinois courts in other cases. *See Des Plaines*, 357 N.E.2d at 436; *Bridgeview*, 8 N.E.3d at 1279.

N.E.2d at 275 (upholding village’s handgun ban because, unlike train noise ordinance in *Des Plaines*, it did not “involve regulation of conduct outside the village of Morton Grove”).<sup>2</sup>

The city also claims that in *Blanchard v. Berrios*, 72 N.E.3d 309, 322 (Ill. 2016), the Supreme Court distinguished *Bridgeview* “because the home rule ordinance ‘affected another unit of local government[.]’” (Opp’n 19.) But the complete sentence from which the city pulled that quote shows the court was also concerned with the ordinance’s extraterritorial effect: “Although their holdings [referring to *Bridgeview* and other cases] do not expressly limit their applicability, the decisions in these cases were premised on the fact that the local ordinances affected another unit of local government *and resulted in an extraterritorial effect.*” *Blanchard*, 72 N.E.3d at 322 (emphasis added).

The city’s citation to *National Waste & Recycling Association v. County of Cook*, 55 N.E.3d 163, 175 (Ill. App. Ct. 2016), is also suspect. Here again the city claims that the court distinguished *Bridgeview* because the ordinance in that case “prohibited residents from operating feral cat colonies . . . in conflict with a Cook County ordinance which permitted such colonies[.]” (Opp’n 19.) But the appellate court actually distinguished *Bridgeview*—and *Des Plaines* too—on the ground that the waste disposal ordinance at issue in *National Waste* did “not impermissibly regulate activities that extend beyond its geographical borders.” 55 N.E.3d at 174-75.<sup>3</sup>

---

<sup>2</sup> The city mistakenly asserts that the Supreme Court in *County of Cook* stated that the municipality in *Des Plaines* sought “to impose its [noise pollution] ordinance on six other municipalities.” (Opp’n 18.) In truth, that quoted language refers to an entirely different case, *Metropolitan Sanitary District v. City of Des Plaines*, 347 N.E.2d 716, 718-19 (Ill. 1976), which involved Des Plaines’ attempt to impose a different health ordinance on a regional sanitary district—despite the city’s misleading insertion of “noise pollution” in brackets inside the quote.

<sup>3</sup> The city’s citations to two other appellate court decisions are equally unavailing. In *Village of Sugar Grove v. Rich*, 808 N.E.2d 525, 531-32 (Ill. App. Ct. 2004), the court upheld several \$50 fines for loud music at a local establishment known as J.R.’s Retreat; the court distinguished *Des Plaines* on the ground that, unlike loud music, the “unwanted noise emissions from the trains were not matters of local concern.” And the city mischaracterizes *Clayton v. Village of Oak*

Finally, the city contends that its 2017 lawsuits against Equifax and Uber show that it has occupied a traditional role alongside the state in regulating this area. (Opp’n 16.) But the city’s new-found use of its ordinance to capitalize on “massive data breaches” betrays the city’s opportunism more than it reflects a traditional regulatory role borne of genuine local concerns. (Am. Compl. ¶ 25.) And it does not nullify the fact that it was the state, and not the city, that traditionally addressed data breaches under the ICFA and PIPA for over a decade.

In sum, from the many cases in which Illinois courts have wrestled with the limits of home-rule authority, three salient factors emerge: where the challenged conduct took place, where the alleged impact took place, and the extent of the state’s expressed interest in the issue. Measured by those factors, the Marriott cyberattack is anything but a Chicago-centric problem.

**B. The City May Not Regulate Conduct Beyond Its Borders.**

Regardless of whether a problem has local ramifications, municipalities have no authority to regulate conduct occurring outside their borders. *See Hertz*, 77 N.E.3d at 609-10; *Commercial Nat’l Bank of Chi. v. City of Chicago*, 432 N.E.2d 227, 243 (Ill. 1982). The city complains this leaves it “powerless to regulate any companies except those whose operations are exclusively within the City borders.” (Opp’n 17.) But what matters is where the challenged conduct occurs, not where the company’s operations are located. The city’s own cases illustrate as much. *See City of Evanston v. Create, Inc.*, 421 N.E.2d 196, 203 (Ill. 1981) (ordinance applied to non-resident owner of rental property in city); *Mulligan v. Dunne*, 338 N.E.2d 6, 15 (Ill. 1975) (non-resident wholesaler required to collect tax on sales of alcoholic beverages made within county).

Allowing this action to go forward would open the door to every other home-rule unit

---

*Park*, 453 N.E.2d 937 (Ill. App. Ct. 1983), as involving “an ordinance with extraterritorial effect” (Opp’n 18), whereas the court described the ordinance at issue there as “affect[ing] only owner-occupied single-family residences within the borders of the village.” 453 N.E.2d at 944.



levying fines (and seeking injunctions or monitoring funds) against every company that falls prey to a “massive data breach.” Contrary to what the city thinks (Opp’n 19), that is the kind of “unrestrained extraterritorial exercise” of home-rule authority the Supreme Court warned against in *Commercial National Bank*, 432 N.E.2d at 243, and again in *Hertz*, 77 N.E.3d at 614.

The city points to its regulation of Marriott’s Chicago hotels as evidence of its home-rule authority here. (Opp’n 17-18.) But though the city may require local hotels to install panic buttons and collect taxes from guests, that does not mean it also can regulate how Marriott handles guest data worldwide. The Supreme Court in *Hertz* rejected the similar notion that “because plaintiffs have business locations in Chicago, they are doing business in Chicago and, because they are doing business in Chicago, the City may require them to collect use taxes on transactions outside of Chicago’s borders[.]” 77 N.E.3d at 613.<sup>4</sup>

Finally, the city points to an Illinois chancery court’s denial of a motion to dismiss in the city’s lawsuit against Uber. (Opp’n 18.) But Uber made only a cursory reference to the home-rule issue in its reply brief—and even then, Uber did not argue that its data breach was not a matter of local concern. (*See* Uber’s Reply in Supp. of Mot. to Dismiss 5-6, Ex. B.) The chancery court’s decision—which has not yet been reviewed by Illinois’s appellate courts—thus has little persuasive value regarding the limits of the city’s constitutional authority here.

## **II. THE CYBERATTACK DID NOT OCCUR PRIMARILY AND SUBSTANTIALLY IN ILLINOIS.**

The city has not alleged a violation of the ICFA in any event, because its complaint makes clear the circumstances relating to the Marriott cyberattack did not “occur primarily and

---

<sup>4</sup> The city states in its response that it is seeking to regulate data security only for Marriott’s Chicago properties. (Opp’n 18.) But the city does not allege that Marriott implemented data security measures in Chicago. Moreover, the amended complaint makes clear that the city seeks to regulate Marriott’s handling of data for Chicago residents who “stay in Marriott’s Chicago hotels *and throughout the country*.” (Am. Compl. ¶ 54) (emphasis added).



substantially in Illinois.” *See Avery v. State Farm Mut. Auto. Ins. Co.*, 835 N.E.2d 801, 853-54 (Ill. 2005). The city counters that it need not prove a violation of the ICFA at all. (Opp’n 19-20.) But the ordinance itself makes compliance with court interpretations under the ICFA “an absolute defense” under the ordinance. Chi., Ill., Mun. Code § 2-25-90(a), (c). The city’s attempt to untether its ordinance from *Avery*’s interpretation of the ICFA therefore fails.<sup>5</sup>

Moreover, the city’s list of purported contacts does not plausibly show the Marriott cyberattack occurred primarily and substantially in Illinois. (Opp’n 20.) The Rule 12(b)(6) record shows that none of the purported “failures” that the city claims led to the attack occurred in Illinois, given that Marriott’s headquarters, and the corporate facilities, data centers, and servers involved were located elsewhere. (*See* Am. Compl. ¶ 51; Br. 2, 11; Defs. Ex. A, at 12-13, ECF No. 33-1.) And the city ignores that its residents provided personal information to stay at Marriott hotels “throughout the country,” not just in Chicago. (Am. Compl. ¶ 54.)

The city’s reliance on cases brought under Illinois’s Biometric Information Privacy Act is misplaced. (Opp’n 21-24.) Those cases were concerned with whether scans of consumers’ faces were “collected” in Illinois, and thus subject to Illinois’s BIPA. *See Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1101-02 (N.D. Ill. 2017); *Patel v. Facebook, Inc.*, 2019 WL 3727424, at \*7 (9th Cir. Aug. 8, 2019) (question of “extraterritoriality requires a decision as to where the essential elements of a BIPA violation take place”). But the issue here—under the ICFA and PIPA—is not the collection of data, but rather whether Marriott implemented “reasonable data security

---

<sup>5</sup> The city’s reliance on *Uber* in this regard is misleading. (Opp’n 19-20.) The chancery court merely stated that the city has the right to sue for ICFA violations via its ordinance, even though it cannot sue under those statutes directly. (Pl. Ex. 2 at 3-4.) The court did not state, however, that the city can prevail on its data breach claims if the ICFA has not been violated or does not apply. Were it otherwise, the city could reach conduct through its ordinance that even the state attorney general could not reach under the ICFA.

measures” *after* information had been collected. (Am. Compl. ¶¶ 80-96.) And as noted just above, the record here shows those data security measures were implemented outside Illinois.

The city also relies on *In re Equifax, Inc. Consumer Data Security Breach Litigation*, 362 F. Supp. 3d 1295, 1334 (N.D. Ga. 2019), which addressed extraterritoriality under a multitude of state statutes in a brief, one-size-fits-all analysis in a 50-page opinion. The court did not mention the ICFA by name in its discussion of extraterritoriality, much less consider *Avery*’s “primarily and substantially” requirement.

The notice and misrepresentation claims fare no better. The city takes issue only with the timing of Marriott’s notice to residents—a decision that the complaint does not (and cannot) pin to Illinois. (Am. Compl. ¶ 107.) And while the city contests the accuracy of Marriott’s online privacy statement, it does not allege the requisite nexus with Illinois. The city suggests, citing *IPOX Schuster, LLC v. Nikko Asset Management Co.*, 191 F. Supp. 3d 799, 808 (N.D. Ill. 2016), and *Sprecht v. Google, Inc.*, 660 F. Supp. 2d 858, 867 (N.D. Ill. 2009), that every online statement necessarily occurs primarily and substantially in every state. But the better view is that merely putting a statement online is not sufficient to meet *Avery*’s “primarily and substantially” standard. *See Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 775 (N.D. Ill. 2008) (dismissing ICFA claim where complaint did not “plausibly suggest that the purported deceptive [Internet] domain scheme occurred primarily and substantially in Illinois”); *see also LG Elec. U.S.A., Inc. v. Whirlpool Corp.*, 809 F. Supp. 2d 857, 861-62 (N.D. Ill. 2011) (nationwide advertising campaign did not occur primarily and substantially in Illinois).

Moreover, the city fails to allege that any Illinois consumer read or was deceived by the privacy statement. This fact distinguishes *Cosmetique, Inc. v. ValueClick, Inc.*, 753 F. Supp. 2d 716, 723 (N.D. Ill. 2010) (8,000 Illinois consumers responded to deceptive online promotion),

and *R. Rudnick & Co. v. G.F. Protection, Inc.*, 2009 WL 112380, at \*2 (N.D. Ill. Jan. 15, 2009) (deceptive “faxes were received by consumers in Illinois”). Indeed, even though the city now claims to have conducted an investigation (Am. Compl. ¶ 10 n.7), it still has failed to identify any resident who was aware of the privacy policy, let alone harmed by it. And while the city argues it need not show deception or injury to state a claim, the absence of such allegations bears heavily on the lack of primary and substantial connection to Illinois. *See Miche Bag, LLC v. Be You, LLC*, 2011 WL 4449683, at \*6 (N.D. Ill. Sept. 26, 2011) (dismissing deceptive trade practices claim under *Avery* because “[a]lthough the misrepresentations in question were made on a website accessible to residents of Illinois, [plaintiff] does not allege that any residents of Illinois actually viewed the website or that it was damaged in the state”).

### **III. THE CITY CANNOT PURSUE A MONITORING FUND ON BEHALF OF ITS RESIDENTS.**

The city argues that suing under its own ordinance automatically gives it standing to request a Marriott-financed monitoring fund. (Opp’n 5-6, 8-9.) But “standing is not dispensed in gross”—instead, it must be established “for each form of relief that is sought.” *Town of Chester v. Laroe Estates, Inc.*, 137 S. Ct. 1645, 1650 (2017) (citation omitted). And as shown in Marriott’s opening brief, municipalities do not have *parens patriae* standing to seek relief on behalf of their residents—which is all the requested monitoring fund (or for that matter its request for injunctive relief) aims to do. (Br. 13-16.)

The city’s own allegations show this fund is purportedly designed to mitigate the alleged impact of the Marriott cyberattack on Chicago residents. The city envisions creating a “more sophisticated surveillance” program that would “alert consumers when, based on reported fraud and other indicators, they need to take immediate action to protect their credit.” (Am. Compl. ¶ 79.) The program is necessary, the city says, because residents face a heightened risk of identity theft and fraud, which they cannot combat on their own. (*Id.* ¶¶ 73-78.) The city now

argues, without any explanation, that the fund would “ensure that Marriott complies with the Ordinance in the future.” (Opp’n 5.) But in truth, the monitoring fund is just another version of the restitution claim that the city sought in its initial complaint and then abandoned.

The city also argues it has a proprietary interest in obtaining its monitoring relief due to its tourism industry. (Opp’n 6-7.) But the city’s attenuated claim that the cyberattack has hurt tourism by discouraging business at Marriott’s local hotels makes no sense—even if guests have not purchased Marriott hotel rooms due to the cyberattack (which the city nowhere alleges has actually occurred), they presumably would just stay at some other Chicago hotel instead. This pretextual rationale only reveals the city’s lack of any legitimate interest in seeking a fund.

Finally, the city claims a propriety interest in “vindicat[ing] the rights of its residents[.]” (Opp’n 7.) But that is just another way of claiming *parens patrie* standing, which the city does not possess. The city cites *City of Milwaukee v. Saxbe*, 546 F.2d 693, 698 (7th Cir. 1976), for the proposition that municipalities have “organizational standing” to assert the rights of their residents, but this court has refused to adopt such a position. *See Prince George’s County v. Levi*, 79 F.R.D. 1, 5 & n.5 (D. Md. 1977); *see also Town of Brookline v. Operation Rescue*, 762 F. Supp. 1521, 1524 & n.6 (D. Mass. 1991) (following this court’s decision in *Levi*). And Illinois likewise has recognized that municipalities lack standing to sue on behalf of their residents. *See City of Wheaton v. Chi. A&E Ry. Co.*, 120 N.E.2d 370, 373-74 (Ill. App. Ct. 1954). If the city could shoehorn its request for a monitoring fund into the rubric of its interest in enforcing its ordinances, then the limits on the city’s *parens patriae* standing would be eviscerated.

### CONCLUSION

The Court should dismiss the amended complaint with prejudice under Rule 12(b)(6) or, alternatively, dismiss its claim for equitable relief under Rule 12(b)(1).

Dated: September 4, 2019

/s/ Daniel R. Warren

Daniel R. Warren  
Lisa M. Ghannoum  
BakerHostetler LLP  
127 Public Square, Suite 2000  
Cleveland, OH 44114  
Tel: (216) 621-0200  
Email: dwarren@bakerlaw.com  
Email: lghannoum@bakerlaw.com

Gilbert S. Keteltas  
Baker & Hostetler LLP  
1050 Connecticut Ave. NW, Suite 1100  
Washington, D.C. 20036  
Tel: (202) 861-1530  
Email: gketeltas@bakerlaw.com

*Attorneys for Defendants*

**CERTIFICATE OF SERVICE**

I hereby certify that on September 4, 2019, the foregoing was filed with the Clerk of Court using CM/ECF, which will send notification to the registered attorneys of record that the document has been filed and is available for viewing and downloading.

/s/ Daniel R. Warren  
*Attorney for Defendants*